Hacia nuevos principios de protección de datos en un nuevo entorno TIC

Dinant, Jean-Marc; Poullet, Yves

Published in:
Internet, derecho y politica

Publication date:
2009

Document Version
le PDF de l'éditeur

Hacia nuevos principios de protección de datos en un nuevo entorno TIC

Yves Poullet con la colaboración de *Jean-Marc Dinant*[*]

Introducción: Un nuevo entorno TIC

1. Internet y, de forma más amplia, la propagación de las TIC en nuestra vida cotidiana (GPS, RFID, móviles) han modificado radicalmente el entorno y han creado nuevos riesgos para nuestra privacidad, considerada ésta en un sentido amplio. En las dos últimas décadas se ha visto una rápida e increíble sucesión de un gran número de innovaciones y tendencias tecnológicas que han desembocado en la formación de una red de telecomunicaciones global. Este desarrollo tecnológico se ha alcanzado a nivel internacional sin que ningún gobierno o movimiento cívico jugase un papel decisivo y sin que los problemas sobre una reducción en la privacidad que acompañan a estas redes hayan sido abordados o resueltos desde el punto de vista técnico.

2. Las características de este entorno se podrían resumir como sigue y, asimismo, se sugiere determinadas metas para garantizar una mejor protección de los ciudadanos que están evolucionando más y más en *"ciudadanos de la red"*.[1]

La red es multifuncional y tiende a enlazar todas las redes de telecomunicación existentes que hasta ahora se mantenían autónomas. La capacidad de la

---

* Reproducción del artículo publicado en *IDP. Revista de Internet, Derecho y Política*, núm. 5 (2007) <http://www.uoc.edu/idp/5/dt/eng/poullet_dinant.pdf>

1 Para una descripción completa podéis leer Y.POULLET; J.M. DINANT (nov. 2004). *Self-determination in an Information Society, Report on the application of Data Protection Principles to the worldwide Telecommunications networks*. Informe para el Comité Asesor de la Convención para la protección de individuos con respecto a procesamiento automático de Datos personales (T-PD). Estrasburgo. Disponible en la página web del Consejo de Europa. El presente artículo es una versión profundamente revisada y resumida de este informe.

infraestructura de comunicación está creciendo y se habla de que alcanzará 10 Kbits/seg.

Con respecto al equipamiento terminal, se observan distintas evoluciones. Primero, el equipamiento terminal, que en los ochenta era unifuncional (el terminal de telefonía de voz para transmisión de señales de audio, la TV. para la transmisión unidireccional de imágenes, etc.), ahora es multifuncional. Con mi portátil puedo enviar correos electrónicos, ver la TV, efectuar transacciones y leer mi periódico. Otra evolución sufrida por el equipamiento terminal es que ya no está anclada a un lugar fijo, sino que nos puede acompañar en nuestros traslados. Por otro lado, su capacidad se está incrementando de forma notable bajo la famosa Ley de Moore. Según esta teoría, cada dieciocho meses, la capacidad de un terminal puede ser doblada por el mismo precio. En otras palabras, tras quince años la capacidad de procesamiento y memoria de los ordenadores se han multiplicado por mil. En concreto, esto significa que la compra de un ordenador en un establecimiento ha sufrido la siguiente evolución:

Año	1987	2005	2020 (x1000)
Procesador	8 Mhertz	3 Ghertz (x 375)	3 TeraHz
Memoria	640KB	512 MB (x 800)	512 Gbytesx
Disco duro	20 Mbytes	120 Gbytes (x 6000)	120 Terabytes
Conexión telefónica	10Kb/seg	3 Mb /seg.	10 Gb/seg.

Para finalizar, también se destaca la tendencia hacia la miniaturización de los terminales gracias al uso de nanotecnología. Los RFID (dispositivos de identificación por radiofrecuencia) son etiquetas o tags llamadas "polvo inteligente". Estos tags pueden estar incrustados en nuestras ropas, en los productos que compramos en supermercados e, incluso, en nuestros cerebros y pueden detectar, controlar y, en última instancia, influir en nuestro comportamiento.

A través del uso de estos diversos terminales, los sistemas informáticos son omnipresentes, ya que han invadido nuestro entorno y todos los segmentos de nuestra vida cotidiana, tanto privada como profesional y, con cada día que pasa, abrirán caminos hacia nuevos campos. Los sistemas de información multiplican las huellas de los usos de los servicios TIC y asimismo multiplican la posibilidad de que determinados controladores de datos hagan un seguimiento de las actividades de los usuarios de Internet.

Muchas de las actividades, que en el pasado se llevaban a cabo sin ninguna red de telecomunicaciones, requerirán de tales redes para ser usadas en el futuro. No es descabellado pensar que, dentro de unos años, la mayoría de neveras estarán equipadas con componentes inteligentes que informarán con exactitud de qué comida está almacenada en ellas y cuándo habrán pasado sus fechas de caducidad (gracias a los chips RFID). Estas neveras "inteligentes" podrán incluso tomar la iniciativa mostrando en el televisor familiar anuncios dirigidos o contactando con los supermercados para obtener ofertas o realizando pedidos de productos. En general, existe una clara tendencia que consiste en crear objetos inteligentes a nuestro alrededor equipándolos con un terminal de telecomunicaciones. Los terminales inteligentes están operando de forma opaca y compleja.

3. En la actualidad, los ordenadores conforman la inmensa mayoría de terminales de telecomunicación. Al estar basados en ordenadores, estos terminales generan, de forma completamente invisible a sus usuarios, muchas huellas de las telecomunicaciones que pasan a través de ellos. Estas huellas se encuentran almacenadas en el terminal o bien se envían a través de la red, habitualmente sin informar al usuario. Los medios técnicos puestos a disposición de los usuarios son incompletos, demasiado complejos y configurados por defecto en un modo perjudicial para la protección de la privacidad de los navegantes de Internet. El respeto a la privacidad se ha convertido en una opción accesible a personas que disponen de tiempo y conocimientos. La relación del individuo con la protección de sus datos se ha convertido en sí en un artículo de información personal que muchos interesados desean poseer.

Los terminales de telecomunicación incorporan diversos identificadores técnicos que permiten "rastrear" el comportamiento del individuo en la red. La mayoría de participantes de la industria no consideran este proceso de rastreo una violación de la privacidad del individuo si éste no puede ser identificado mediante un punto de contacto. La tecnología de los cookies permite que una página web, por defecto, inserte con disimulo su propio identificador en el terminal de forma permanente para poder así rastrear el comportamiento del individuo en Internet.

4. Los protocolos de telecomunicaciones y el funcionamiento de los terminales no incluyen la protección de datos como requisito clave, sino como una opción generalmente dejada a la discreción de los fabricantes de dispositivos y programas que incorporan estos estándares.

Determinadas opiniones expresadas recientemente por el Grupo del Artículo 29 han argumentado que el principio establecido por el considerando 2 de la Directiva 95/46 UE sobre protección de datos, que afirma claramente que la tecnología debe servir en beneficio de los individuos y la sociedad, puede considerarse una justificación para imponer a los fabricantes de equipamiento terminal (incluyendo elementos de programas incorporados en los terminales) determinadas obligaciones dirigidas hacia la transparencia de su funcionamiento y prevenir el uso injusto o ilícito de datos personales asociados a la conexión y la comunicación con redes. Se debe observar que estos fabricantes no están cubiertos como tales por la presente directiva, ya que no son los controladores de un archivo. Sin embargo, como el diseño del equipamiento que ellos proveen autoriza muchas operaciones de procesamiento, se les debería imponer determinadas responsabilidades sobre seguridad para prevenir esas operaciones que podrían realizar terceras partes de forma injusta o ilícita, y deberían ser exigibles para garantizar la transparencia, ya que el usuario del terminal debe poder ejercitar un determinado control sobre los flujos de datos generados mediante su uso.

5. Finalmente, podemos resaltar el carácter global de Internet. Debido a la naturaleza global de las redes modernas y a la ausencia de fronteras con respecto a la infraestructura, el procesamiento operado por personas localizadas fuera de las fronteras nacionales puede afectar directamente nuestra privacidad mediante el envío de spyware, transmitiendo datos a terceras partes a través de hiperenlaces invisibles o dirigiendo correo no solicitado a través de la web, etc. La abolición de fronteras nacionales hace necesaria una aproximación común hacia los principios de protección de datos y su posible imposición más allá de las fronteras. El WSIS (World Summit on the Information Society) se ha declarado a favor de un reconocimiento internacional de la protección a la privacidad.

Algunos principios nuevos para promover la autodeterminación de la información en el nuevo entorno tecnológico

6. Esos rasgos que son los más característicos del entorno del servicio de comunicaciones electrónicas –presencia creciente y multifuncionalidad de las redes y terminales de comunicación electrónica, su interactividad, el carácter internacional de las redes, servicios y productores de equipamiento y la ausencia de transparencia en el funcionamiento de terminales y redes– incrementan el riesgo de infringir las libertades individuales y la dignidad humana.

Para contrarrestar estos riesgos deben establecerse algunos nuevos principios si se desea que los interesados estén mejor protegidos y que tengan mayor control sobre su entorno. Dicho control es esencial si los usuarios van a ejercitar una responsabilidad efectiva para su propia protección y deben estar mejor preparados para ejercitar apropiadamente la autodeterminación de la información.

Éste es el primer intento de esbozo de tales principios. Está basado en una diversidad de documentación y hemos tratado de estructurarlo en torno a cinco principios clave, ya que en este estadio preferimos no hablar de nuevos "derechos" para el interesado. Su contenido y extensión debería ser discutido por otros interesados y podrían entonces, si es apropiado, formar las bases para recomendaciones y otras medidas ad hoc para dotarles de mayor fuerza.

a. Primer principio: El principio de encriptación y anonimato reversible

7. La encriptación de mensajes ofrece protección contra el acceso al contenido de las comunicaciones. La calidad varía al hacerlo las técnicas de encriptación y desencriptación. Ahora se encuentran disponibles, a precios razonables, programas de encriptación para su instalación en los ordenadores de los usuarios de Internet (protocolos S/MIME u Open PG). Mientras tanto, dada su ambigüedad, la noción de anonimato debería quizás ser clarificada y, posiblemente, sustituida por otros términos como "pseudoanonimato" o "no-identificable". Lo que se busca no es siempre el anonimato absoluto, sino la no-identificación funcional del autor de un mensaje enviado a otras personas.[2] Existen

2 Véase J. GRIJPINK; C. PRIENS (2001). "Digital Anonymity on the Internet, New Rules for Anonymous Electronic Transactions?". *Computer Law & Security Report*. Vol. 17, n.° 6, pág. 379-389.

muchos documentos no vinculantes[3] defendiendo el "derecho" al anonimato de los ciudadanos cuando utilizan servicios de nueva tecnología. La recomendación núm. R (99) 5[4] del Comité de Ministros del Consejo de Europa establece que "el acceso y uso anónimo de servicios y medios anónimos de realizar pagos son las mejores protecciones de la privacidad", de ahí la importancia de las técnicas de potenciación de privacidad ya disponibles en el mercado.

El primer principio referido a la no identificación funcional podría ser expresado como sigue: Aquellos que usen técnicas modernas de comunicación deben poder permanecer no identificados por los proveedores de servicios, por otras terceras partes que intervinieran durante la transmisión del mensaje y por el receptor o receptores del mensaje, y deberían tener acceso gratis, o a precios razonables, a los medios de ejercitar esta opción.[5] La disponibilidad de encriptación económica y herramientas y servicios para mantener el anonimato es una condición necesaria para internautas que ejerzan su responsabilidad personal.

Sin embargo, el anonimato o la "no identificación funcional" requerida no es absoluta. El derecho del ciudadano al anonimato debe ser establecido en oposición a intereses mayores de Estado, el cual podría imponer restricciones si fuesen necesarias *"para proteger la seguridad nacional, defensa, seguridad pública, [y para] la prevención, investigación, detección y persecución de delitos"*. Lograr un equilibrio entre la monitorización legítima de delitos y la protección de datos debería ser posible mediante el uso de "pseudo-identidades" que serían asignadas a individuos mediante proveedores de servicios especializados que podrían ser requeridos para revelar la identidad real de un usuario pero sólo en determinadas circunstancias y siguiendo procedimientos claramente establecidos por la ley.

8. Se podrían extraer otras consecuencias de este primer principio: podría incluir la regulación exigida de equipamientos terminales, para prevenir la monitorización de la navegación, para permitir la creación de direcciones efímeras y para la diferenciación de datos de direcciones según qué terceras partes tendrían acceso al dato de tráfico o localización, y para la desaparición de los identifica-dores únicos globales mediante la introducción de protocolos de direcciones uniformes.

Finalmente, el estatus de "anonimizador", en el que aquellos que lo usan depositan gran confianza, debería estar regulado para ofrecer a los afectados determinadas barreras con respecto al estándar de servicio que proporcionan, a la vez que garantizasen que el Estado posea los medios técnicos para acceder a las telecomunicaciones en circunstancias legalmente definidas.[6]

b. Segundo principio: El principio de beneficios recíprocos

9. Donde fuese aplicable, este principio haría que aquellos que empleen nuevas tecnologías tuviesen la obligación legal de desarrollar su actividad profesional con el fin de aceptar determinados requisitos para reestablecer el equilibrio tradicional entre las partes implicadas. La justificación es simple, si la tecnología incrementa la capacidad de acumulación, procesamiento y comunicación de información sobre terceros y facilita las transacciones y operaciones administrativas, es esencial que también esté configurada y empleada para garantizar que los interesados, tanto si son ciudadanos como consumidores, disfruten de un beneficio proporcional de estos avances.

Varias previsiones recientes se han inspirado en el requisito proporcional para obligar a que aquellos que emplean tecnologías tengan que ponerlas a disposición de los usuarios para que puedan hacer valer sus intereses y derechos.

Un ejemplo es la Directiva Europea 2001/31/CE (la "Directiva de E-Comercio"), que incluye previsiones electrónicas anti-spamming. De forma

3 Véase en particular S. RODOTÀ. "Beyond the E.U. Directive: Directions for the Future". En: Y. POULLET; C. DE TERWANGNE; P. TURNER (ed.). "Privacy: New Risks and Opportunities". *Cahier du CRID*. Amberes: Kluwer. N.° 13, pág. 211 f.

4 Se encuentran disponibles varias recomendaciones para la protección de individuos con respecto a la recaudación y procesamiento de datos personales en las autopistas de la información en el sitio del Consejo de Europa. Ver también Recomendación 3/97 del llamado Grupo del Artículo 29: Anonimato en Internet, y la opinión de la comisión privada belga sobre comercio electrónico (N.° 34/2000 del 22 de noviembre de 2000, disponible en el sitio de la comisión: http://www.privacy.fgov.be), que apunta que existen tres modos de identificar los remitentes de mensajes sin que necesariamente se les requiera su identificación.

5 Ver la recomendación de la comisión de procesamiento de datos nacionales franceses que el acceso a páginas comerciales debería ser siempre posible sin identificación previa: M. GEORGES (2000). "Relevons les défis de la protection des données à caractère personnel: l'Internet et la CNIL". *Commerce électronique-Marketing et vie privée*. París. Pág. 71 y 72.

6 Se podrían establecer los requisitos para los servicios proporcionados y con respecto a la confidenciabilidad, como se propone para las firmas digitales. La aprobación oficial de un anonimizador indicaría que se cumplen los requisitos. Tal aprobación oficial podría ser voluntaria más que obligatoria, como en el caso de etiquetas de calidad.

similar, el artículo 5.3 de la Directiva 2002/58/CE sobre comunicaciones privadas y electrónicas incluye, incluso, el requisito de que *"...el uso de redes de comunicación electrónicas con el fin de almacenar información u obtener acceso a la información almacenada en el equipamiento terminal de un suscriptor o usuario tan sólo está permitido bajo la condición de que al suscriptor o usuario implicado se le haya proporcionado información clara y comprensible (...) y se le ofrezca el derecho a rechazar dicho procesamiento (...)"*. El derecho de los suscriptores, bajo el artículo 8.1, "a través de medios simples, libres de cargo alguno, eliminar la presentación de identificación de línea telefónica en términos de llamada (...) y en términos de línea" es otra aproximación potencialmente valiosa si el concepto de "línea telefónica" se amplía a diversas aplicaciones de Internet, tales como servicios web y correo electrónico.[7] Esto implica una obligación relacionada del proveedor de servicios hacia los usuarios consistente en ofrecerle las opciones de rechazar o aceptar llamadas no identificadas o prevenir su identificación (artículos 8.2 y 8.3).

10. Las legislaciones llamadas "Libertad de Información" introduce un derecho similar de transparencia con respecto al Gobierno mediante la adición de mayor información que este último tiene obligación de suministrar. Un desarrollo bien recibido en el Reino Unido es la introducción reciente de una garantía de servicio público en el manejo de datos.[8] Recientemente, una comisión sueca[9] ha recomendado una legislación que daría derechos a los ciudadanos para monitorizar sus casos electrónicamente de inicio a fin, incluyendo su archivo, y obligaría a las autoridades a adoptar una buena estructura de acceso pública, para facilitar a los individuos la identificación y localización de documentos específicos. Existe incluso un borrador de legislación que haría posible, de un modo u otro, enlazar cualquier documento oficial en el que se basasen las decisiones a otros documentos del caso. En otras palabras, un servicio público que se ha tornado más eficiente gracias a las nuevas tecnologías debe ser también más transparente y accesible para los ciudadanos. El derecho de acceso de los ciudadanos se extiende más allá de los documentos que les conciernen directamente para incluir las normativas sobre las que se basó la decisión.

11. Es incluso posible imaginarse que determinados derechos asociados a la protección de datos, como el derecho a la información, los derechos de acceso y rectificación y el derecho a la reclamación, podrían ser de obligado cumplimiento electrónicamente. Se podrían proponer muchas aplicaciones:

- Debería ser posible aplicar el derecho a la información de los interesados en cualquier momento mediante un simple clic (o de forma más generalizada mediante una acción electrónica e inmediata) ofreciendo el acceso a la política de privacidad, que debería ser tan detallada y completa como permita el menor coste de la propagación electrónica. Dicho paso debe ser anónimo con respecto al servidor de la página, para evitar así cualquier riesgo de creación de archivos sobre usuarios "preocupados por la privacidad". Además, en el caso de páginas a las que se han otorgado etiquetas de calidad, debería ser obligatorio que proporcionasen un hiperenlace desde el símbolo de la etiqueta hacia el organismo que le ha otorgado la etiqueta. Lo mismo sería aplicable a la declaración del controlador del archivo hacia la autoridad supervisora. Se instalaría un hiperenlace entre una página ineludible de cualquier sitio web con procesamiento de datos personales y la autoridad supervisora relevante. Finalmente, se podría prestar atención a la señalización automática de cualquier página localizada en un país que ofreciese una protección inadecuada.
  En el futuro, los interesados deberían poder ejercitar su derecho de acceso empleando una firma electrónica. Sería obligatorio estructurar los archivos para que el derecho de acceso fuese de fácil aplicación. La información adicional debería estar sistemáticamente disponible, como el origen de los documentos y un listado de los interesados a los que se les habría suministrado determinados datos. Como se ha mencionado anteriormente,[10] de

7 Obsérvese la conexión entre estas previsiones y el principio de anonimato.

8 Garantía de servicio público en el manejo de datos: disponible ahora para su implementación en entidades públicas. De este modo se establecen los derechos de las personas sobre cómo son manipulados sus datos personales y los estándares que pueden esperar que las organizaciones publicas suscriban. http://www.dca.gov.uk/foi/sharing/psguarantees/data.htm#2

9 P. SEIPEL (2004). "Information System Quality as a Legal Concern". En: U. GASSER (ed.). *Information Quality Regulation: Foundations, Perspectives and Applications*. Nomos Verlagsgesellschaft. Pág. 248. Véase también el informe de la comisión sueca de P. SEIPEL (2002). *Law and Information Technology: Swedish Views*. Swedish Government Official Reports, SOU. Pág. 112.

10 Ver párrafo 3.

forma incremental, los datos personales acumulados por un gran número de público y de redes privadas no se guardan con uno o más propósitos claramente definidos, sino que se almacenan en la red para usos posteriores que sólo emergen según surgen nuevas oportunidades de procesamiento o necesidades no identificadas previamente. En tales circunstancias, los interesados deben poder tener acceso a la documentación que describen los flujos de datos en la red, los datos concernientes y los diversos usuarios –un tipo de registro de datos.[11]

- Debería ser posible ejercitar en línea los derechos de rectificación y/o impugnación a una autoridad con un estatus claramente definido responsable de mantener o considerar un listado de quejas.
- El derecho a la reclamación debería también beneficiarse de la posibilidad de derivación en línea, intercambio de solicitudes de las partes y otras documentaciones, decisiones y proposiciones de mediación.
- Finalmente, cuando los individuos interesados deseen apelar las decisiones tomadas automáticamente o notificar mediante una red (como el rechazo a otorgar un permiso de construcción tras un llamado procedimiento e-gubernamental), deberían tener derecho a la información, mediante el mismo canal, sobre la lógica subyacente en la decisión. Por ejemplo, en el sector público[12] los ciudadanos deberían tener el derecho a probar de forma anónima cualquier paquete de toma de decisiones o sistemas expertos que pudiesen utilizar. Esto se podría aplicar a los programas para el cálculo automático de impuestos o derechos a subsidios para la rehabilitación de viviendas.

11 Esta idea es el origen de dos leyes belgas recientes que requieren el establecimiento de comités sectoriales para las redes enlazadas al Registro Nacional (Acta del 8 de agosto de 1983 que establece un registro nacional de personas, según las amiendas del Acta del 35 de marzo de 2003, MB 28 de marzo de 2003, art. 12§1) y a la autoridad de registro comercial (Banque Carrefour des entreprises) (Acta de 16 de enero de 2003 estableciendo la autoridad, MB 5 de febrero 2003, artículo 19 §4).

12 Se aplica el mismo principio a los tomadores privados de decisiones, sujetos a los intereses legítimos de los controladores de archivo (especialmente relacionado a la confidenciabilidad de empresas, que podría limitar la obligación de clarificar la lógica subyacente).

c. Tercer principio: El principio al fomento de aproximaciones tecnológicas compatibles con la situación de personas protegidas legalmente o su mejora

12. Recomendación 1/99 del llamado Grupo del Artículo 29 (grupo de trabajo sobre protección de datos de la UE),[13] que se preocupa de la amenaza a la privacidad presentada por los programas y maquinaria de comunicaciones en Internet, establece el principio de que la industria de productos de programas y maquinaria debería proporcionar las herramientas necesarias para acatar las normas europeas de protección de datos. Según este tercer principio, a los reguladores se les debería otorgar diversos privilegios. Esta conclusión se ha deducido del considerando 2 de la Directiva 95/46 sobre protección de datos que prevé que los sistemas de información y los productos deben estar al servicio de la sociedad y de los individuos.

Por ejemplo, los reguladores deberían poder intervenir en respuesta a desarrollos tecnológicos que presente riesgos importantes. El llamado principio de precaución, que se encuentra bien establecido en las leyes ambientales, también podría aplicarse a la protección de datos. El principio de precaución podría requerir que el equipamiento terminal de telecomunicaciones (incluyendo los programas) adoptasen los parámetros más protectores como opción por defecto para garantizar que aquellos afectados no estén, por defecto, expuestos a los diversos riesgos de los que no tienen conocimiento y que no podrían evaluar.

De forma similar, según el principio de beneficios recíprocos, es apropiado y nada irracional equipar los terminales de telecomunicación con weblogs (blogs), como es el caso de programas tipo servidor usados por compromisos en línea y departamentos gubernamentales. Esto permitiría que los usuarios controlasen qué personas han accedido a su equipo y, cuando fuese apropiado, identificar las características principales de la información transferida.

13. Este principio puede ilustrarse con una provisión de la Directiva de la UE sobre privacidad y comunicaciones electrónicas. El artículo 14 establece que donde se requiera, la Comisión puede adoptar medidas que garanticen que el equipo terminal es compatible con las normas de protección de datos. En otras palabras, la estandarización de equipamiento terminal es otra manera, cierta-

13 Grupo del Artículo 29. Recomendación sobre el procesamiento invisible y automático de datos personales a través de Internet llevado a término mediante programas o maquinaria

mente subsidiaria, de protección de datos personales de los riesgos de procesamiento ilegal –riesgos que han sido creados por todas estas opciones de nueva tecnología. Yendo más lejos, es necesario prohibir las llamadas tecnologías para acabar con la privacidad,[14] según el principio de seguridad consagrado en el artículo 7 del Convenio 108 del Consejo de Europa. La obligación de introducir medidas técnicas y organizativas apropiadas para contrarrestar las amenazas hacia la privacidad de datos requerirá que los administradores de sitios se aseguren de que el intercambio de mensajes permanezca confidencial, y que también se indique claramente qué datos están siendo transmitidos, bien de forma automática o mediante hiperenlace, como es el caso de compañías de cibermercadotecnia.

Esta obligación de seguridad también requerirá que aquellos que procesan datos personales opten por la tecnología más apropiada para minimizar o reducir la amenaza a la privacidad. Este requisito tiene una clara influencia sobre el diseño de tarjetas inteligentes, en particular sobre tarjetas multifuncionales,[15] como las tarjetas de identificación. Otro ejemplo de la aplicación de este principio afecta a la estructura de archivos médicos a diversos niveles, como recomienda el Consejo de Europa.

14. Se podría ir más lejos recomendando, tal y como ha hecho recientemente el Comité de la UE (2 de mayo de 2007), el desarrollo de tecnologías que potencien la privacidad, refiriéndose a herramientas o sistemas que pongan mayor énfasis en los derechos de los interesados. Por descontado, el desarrollo de estas tecnologías dependerá del libre comportamiento del mercado, pero el Estado debe tomar una postura activa para potenciar productos que sean compatibles con la privacidad y que la cumplan, ofreciendo subsidios de investigación y desarrollo, estableciendo certificaciones voluntarias y sistemas de acreditación equivalentes, publicitando sus etiquetas de calidad y garantizando que

14 Expresión utilizada por J. M. DINANT en "Law and Technology Convergence in the Data Protection Field?". En: I. WALDEN; J. HORNE (2002). *E-commerce Law and Practice in Europe*. Cambridge: Woodhead Publishers. Cap. 8.2.

15 Sobre diseños de tarjetas multi-aplicación que satisfacen la privacidad, véase E. KEULEERS; J.M. DINANT (2004). "Data protection: multi-application smart cards. The use of global unique identifiers for cross-profiling purposes". Parte 2: "Towards a privacy enhancing smart card engineering". En: *Computer Law and Security Report*. Oxford: Elsevier. Vol. 20, n.° 1, pág. 22-28.

aquellos productos que se consideren necesarios para la protección de datos estén disponibles a precios razonables.

d. Cuarto principio: El principio de que el usuario mantenga pleno control sobre el equipamiento terminal

15. La justificación para este principio es obvia. Dado que estos terminales pueden permitir que otros monitoricen nuestras acciones y comportamiento, o simplemente nos localicen, deben funcionar de forma transparente y bajo nuestro control. El artículo 5.3 de la Directiva 2002/58/EC, citado anteriormente, ofrece una primera ilustración sobre este punto. Los interesados deben ser informados sobre cualquier acceso remoto a sus terminales mediante cookies, spyware u otros medios y deben tener la posibilidad de tomar contramedidas fáciles, efectivas y libres de cargo alguno. La Directiva 2002/58/EC también establece la norma de que los usuarios de líneas conectadas y emisores de llamadas puedan prevenir la presentación de la identificación de línea llamante.

Más allá de los anteriores ejemplos, podríamos argumentar que todo equipo terminal debería ser configurado de forma que garantice que los propietarios y usuarios tienen información completa sobre cualquier flujo de datos entrantes o salientes para que puedan así realizar las acciones que consideren apropiadas. De forma similar, como es ya el caso bajo determinada legislación, la posesión de una tarjeta inteligente debería estar acompañada por la posibilidad de acceder a la lectura de los datos almacenados en la tarjeta.

16. El control ejercido por el usuario también significa que los individuos pueden decidir desactivar sus terminales de forma definitiva y en cualquier momento. Esto adquiere importancia con respecto a los identificadores por radiofrecuencia (RFID). Los interesados deben tener la posibilidad de confiar en terceros[16] que garanticen que dichos medios técnicos de identificación remota han sido completamente desactivados.

Los usuarios bien podrían aplicar este principio a empresas que no se encuentran necesariamente cubiertas por las normas de protección de datos, ya

16 Con certeza se refiere a acuerdos de acreditación como los descritos ya en el párrafo 15 (regulación conjunta) o la emisión, por parte de las autoridades, de autorizaciones para realizar determinadas acciones (regulación pública).

que no son responsables del procesamiento de datos. Algunos ejemplos incluyen suministradores de equipo terminal y muchas formas de programas de navegación que pueden incorporarse a los terminales para facilitar la recepción, el procesamiento y la transmisión de comunicaciones electrónicas.

Este principio también se aplica a organismos de ordenación estándar públicos y privados preocupados por la configuración de dicho material y equipamiento.

17. El punto clave radica en que los productos suministrados a los usuarios no deberían estar configurados de tal forma que pudiesen ser usados, bien por terceras partes o por los fabricantes en sí, para propósitos ilícitos. Se puede ilustrar con varios ejemplos:

- Una comparación de los navegadores disponibles en el mercado muestra que el diálogo que intercambian sobrepasan en gran medida lo que sería estrictamente necesario para establecer la comunicación.[17]
- Entre los navegadores existe gran diversidad sobre cómo reciben, eliminan y previenen el envío de cookies, lo que implica que las oportunidades de procesamiento inapropiado también variarán de un navegador a otro. Sin embargo, parece ser imposible, al menos de modo simple, que en el navegador por defecto instalado en la mayoría de los cientos de millones de ordenadores personales bloquee las ventanas emergentes o la comunicación sistemática de referencias a artículos leídos en línea o a palabras clave introducidas en los motores de búsqueda.
- También se debe prestar atención al uso que hacen los suministradores de herramientas de navegación y programas de comunicación sobre identificadores únicos y spyware.

18. De forma generalizada, el equipamiento terminal debería funcionar de manera transparente para que los usuarios mantuviesen un control completo sobre los datos enviados y recibidos. Por ejemplo, debería ser posible establecer, sin complicaciones, la extensión precisa del diálogo en sus ordenadores, qué archivos se han recibido, sus propósitos y quién los envió o recibió. Bajo ese punto de vista, los blogs parecen ser una herramienta apropiada que es relativamente fácil de introducir.

17 Ver Jean-Marc DINANT (invierno, 2001). "Le visiteur visité". *Lex Electronica*. Vol. 6, n.° 2.

19. Además del derecho del usuario a ser informado sobre los flujos de datos entrantes, existe la cuestión sobre si las personas tienen el derecho de requerir a terceros la obtención de autorización para penetrar en su "hogar virtual". En este punto es relevante el Convenio del Consejo de Europa sobre cibercrimen, en particular los artículos 2 (acceso ilegal)[18] y 3 (intercepción ilegal).[19] En este caso, la identificación de las personas que tienen parte activa en las comunicaciones no es una precondición para la aplicación del convenio. De forma similar, el acceso no autorizado a un sistema informático no está limitado al pirateo de grandes sistemas operados por bancos o departamentos gubernamentales, sino también a accesos no autorizados a terminales de telecomunicación, estando éstos representados en la situación tecnología actual por los ordenadores.[20]

En otras palabras, mantenemos que situar un número de identificación en un terminal de telecomunicación o acceder simplemente a este número u otro identificador de terminal, constituye un acceso no autorizado. En tal contexto legal, no puede existir duda en la evaluación de proporcionalidad de dichas acciones. La autorización es un acto positivo, bastante distintivo a cualquier aceptación que pudiera ser inferida del silencio o de no expresar objeción.

Por lo tanto no se puede dar por asumido, como hizo DoubleClick,[21] que

18 Artículo 2 - Acceso ilegal: Cada parte adoptará las medidas necesarias, bien legales o de otra naturaleza, para que bajo la ley local queden establecidas como ofensas criminales el acceso a cualquier parte o a todo el sistema informático sin tener derecho, cuan do se hubiesen cometido intencionalmente. Una Parte podría requerir que la ofensa fuese cometida mediante la infracción de medidas de seguridad, con la intención de obtener datos informáticos u otra intención deshonesta, o en relación a un sistema informático conectado a otro sistema informático.

19 Artículo 3 - Acceso ilegal: Cada parte adoptará las medidas necesarias, bien legales o de otra naturaleza, para que bajo la ley local queden establecidas como ofensas criminales, cuando habiendo sido cometidas de forma intencional, la intercepción sin derecho, realizada a través de medios técnicos, de transmisiones privadas de datos informáticos, desde un sistema informático o en él, que incluyan emisiones electromagnéticas desde un sistema informático transmisor de dichos datos informáticos. Una Parte podría requerir que la ofensa fuese cometida con intención deshonesta, o en relación a un sistema informático que estuviese conectado a otro sistema informático.

20 En este contexto véase el excelente artículo de Thierry LEONARD. "E-commerce et protection des données à caractère person-nel: Quelques considérations sur la licéité des pratiques nouvelles de marketing sur internet". Disponible en: http:// www.droit.fundp.ac.be/Textes/Leonard1.pdf

21 A consecuencia de la demanda colectiva iniciada contra ellos hace varios años en Estados Unidos, la práctica actual de Double-Click es enviar a todos los terminales no identificados una cookie inicial no residual y no identificadora llamada "aceptar cookies". Si la *cookie* es retornada, DoubleClick asume que el terminal acepta las cookies, y envía una cookie identificadora que se mantiene durante unos diez años (anteriormente treinta). Si no se retorna la cookie, DoubleClick enviará indefinidamente la cookie requiriendo autorización. Está disponible una opción de exclusión que permite a los usuarios informados almacenar una cookie que tiene el significado de que no las acepta.

por el mero hecho de no activar el supresor de cookies, los usuarios hayan otorgado su autorización plena a la instalación de este tipo de información en sus terminales.

e. El principio de que los usuarios de determinados sistemas de información deberían beneficiarse de la legislación de protección al consumidor

20. El uso rutinario de tecnologías de la información y comunicación, anteriormente confinado a actividades trascendentales, y el rápido desarrollo del comercio electrónico que ha multiplicado el número de servicios en línea han conducido a una aproximación más consumista de la privacidad. Los navegantes de Internet ven incrementadas las transgresiones hacia su privacidad –*spamming*, creación de perfiles, políticas de cargos diferenciados, rechazo de acceso a determinados servicios, etc.– desde la perspectiva de los consumidores de estos nuevos servicios.

De este modo, en Estados Unidos los primeros pasos indecisos hacia la legislación de la protección de datos en el sector privado se enfocó en la protección del consumidor en línea. Ya se ha hecho referencia a la legislación califor-niana,[22] pero también deberíamos tener en cuenta la Ley de Privacidad del Consumidor de 1995 y, más recientemente, la declaración del 2000 de la Comisión de Comercio Federal,[23] que enfatiza la necesidad de legislación de privacidad para la protección de los consumidores en línea. En Europa y en América, las medidas para combatir el *spamming* se preocupan tanto de los intereses económicos de los consumidores como de los datos de privacidad de los sujetos.

21. Esta convergencia entre los intereses económicos de los consumidores y las libertades de los ciudadanos abre perspectivas interesantes. Sugiere que el derecho a recurrir a determinadas formas de acción colectiva, que ya están reconocidas en el campo de protección al consumidor, debería extenderse a asuntos de privacidad. Dicho derecho a "demandas colectivas" es particularmente relevante en un área en la que a menudo es difícil evaluar el perjuicio

22 Ver párrafo 12.

23 Ver el informe para el Congreso "Privacidad en línea: Prácticas de Información Justas" de mayo del 2000, disponible en el sitio FTC: http://www.ftc.gov/os /2000/05/index.htm. En Estados Unidos, el FTC, que es muy activo en el campo de la protección al consumidor, ha jugado un papel clave en la protección a la privacidad de los ciudadanos.

sufrido por los interesados y en el que el bajo nivel de daños concedidos es un desánimo a las acciones individuales.

Además, existen muchos aspectos de la ley del consumidor que podrían aplicarse eficazmente a la protección de datos. Algunos ejemplos serían las obligaciones de proporcionar información y asesoramiento, que podrían imponerse a los operadores que ofrecen servicios que implican esencialmente la gestión y suministro de datos personales, tales como los proveedores de acceso a Internet y servidores de bases de datos personales (bases de datos de jurisprudencia, motores de búsqueda y similares), la ley aplicable a las condiciones generales de la contratación (aplicable a política de privacidad) y medidas para combatir prácticas comerciales y competencia desleal.

Para finalizar, proporcionar datos personales como condición de acceso a un sitio web o a un servicio en línea podría ser visto no sólo bajo la perspectiva de la legislación de protección de datos –¿el consentimiento del usuario cumple los requisitos necesarios? y ¿es suficiente para legalizar el procesamiento en cuestión?– sino también bajo la legislación sobre defensa del consumidor, aunque sólo fuese en términos de prácticas injustas en la obtención de consentimiento o de obstáculos importantes surgidos del desequilibrio entre el valor de la seguridad de datos y el de los servicios suministrados.

Otro camino que hay que explorar es si la responsabilidad del producto de terminales y software puede hacerse extensiva más allá de la causación de un daño físico o económico para poder incluir la vulneración de los requisitos de protección de datos. ¿Hasta qué punto un suministrador de un navegador cuyo uso induce a vulnerar la intimidad es responsable objetivo por la violación de la normativa sobre protección de datos causada por un tercero?

Conclusiones

22. La irrupción de Internet ha creado la necesidad de una tercera generación de regulaciones sobre protección de datos. No se trata de volver la espalda a las dos primeras generaciones, sino de proporcionar un nivel adicional de protección, manteniendo inalteradas las medidas ya introducidas. La primera

generación estaba principalmente basada en la naturaleza de los datos, en esencia, en si eran sensibles y si afectaban al dominio privado de los individuos. La autodeterminación informativa fue entonces equiparada con la prohibición de procesamiento de dichos datos, y se englobó en el artículo 8 de la Convención Europea de Derechos Humanos. La segunda generación se ocupaba no sólo de la protección de datos personales, sino también del modo en la que su procesamiento podría modificar el equilibrio de poder entre los procesadores de información y los sujetos de ese procesamiento. La autodeterminación informativa fue así extendida para ajustar este equilibrio mediante la garantía de que dicho procesamiento permanecería transparente y se restringiría el derecho a procesar datos sobre terceros. Éste fue el origen de la Convención N.° 108. Tiene muchos emuladores y ha justificado su existencia ampliamente.

23. La tercera generación emergente, que esperamos se adopte con rapidez, se caracteriza por su reconocimiento de la tecnología en sí misma. El uso de las nuevas tecnologías multiplica la cantidad de datos y de los individuos capaces de acceder a ellos, incrementa el poder de aquellos que las recopilan y procesan, y rompe fronteras. Otro factor a tener en consideración es la complejidad y opacidad de esta tecnología. Un tercer implicado –sea el terminal o la red– interviene ahora entre el individuo y el controlador de datos. La autodeterminación informativa reclama una medida de control sobre este tercer implicado.

¿Cómo debería ejercitarse este control? Las sugerencias siguientes no son exhaustivas en el tema:

- "La respuesta a la máquina reside en la máquina" según Clarke,[24] en relación con los problemas que la sociedad de la información plantea a la propiedad intelectual. También podría sugerir vías de afrontar las amenazas que la misma sociedad presenta a la privacidad. Como ya se ha visto, el principio de beneficios recíprocos y la promoción de aproximaciones tecnológicas con "mentalidad privada" pueden ayudar a aquellos interesados en ejercitar un mayor control sobre la circulación y uso de su información personal.
- Este optimismo tiene sus límites. Aunque estas tecnologías podrían contribuir a lo que algunos llaman "empoderamiento" o "dar poder" al usuario, existe el riesgo de que a los individuos afectados se les deje hacer frente sin apoyo a los controladores de datos. En realidad, la tecnología no es neutral: aunque es ampliamente ofertada a los ciudadanos, continúa estando indirectamente financiada por las empresas y las agencias y departamentos oficiales que pagan los servidores. Inevitablemente, estos últimos están probablemente más atentos a los intereses de los controladores de datos que a los de los interesados. La llamada tecnología de protección de la privacidad transforma o podría transformar la relación entre los individuos y sus propios datos personales convirtiéndola en una relación de propiedad que, gracias a las nuevas tecnologías, se convierte en negociable. Por lo tanto es necesario destacar que la autodeterminación informativa es una libertad personal que en absoluto es susceptible de negociación y que la sociedad tiene la obligación de fijar ciertos límites al derecho de usar esos datos.
- Este enfoque sobre las herramientas tecnológicas debe también extenderse a nuevos jugadores ajenos al ámbito de la legislación de la segunda generación, principalmente a los servicios de comunicación y suministradores de equipos terminales. Su papel es crítico en cualquier intento de permitir que los usuarios de los nuevos servicios de la sociedad de la información monitoricen los datos entrantes y salientes del sistema, además de las huellas de datos que ofrecen a las redes y sus posibles usos. Se deben establecer responsabilidades estrictas en el suministro de equipamiento y servicios que cumplan con la privacidad.

24. ¿Qué quiere decir exactamente esta responsabilidad de los productores de equipos terminales y de suministros de servicios de comunicación? En nuestra opinión, los proveedores de acceso a Internet, móviles y otros operadores telefónicos son los responsables de informar al público sobre los riegos asociados al uso de sus redes, informando sobre tecnologías amenazadoras de la privacidad y de ofrecer acceso a aplicaciones apropiadas para favorecer la privacidad. Estos proveedores de acceso tienen un papel central, ya que actúan de guardabarreras entre los usuarios y la red. Por lo tanto se les pide[25] "informar a los usuarios sobre medios técnicos que puedan usar legítimamente para redu-

24 C. CLARKE (1996). "The answer to the machine is in the machine". En: B. HUGENHOLTZ (ed.). *The Future of Copyright in a Digital Environment*. Kluwer. Pág. 139 f.

25 Recomendación del Consejo de Europa R (99) 5, III, 1, 2 y 4.

cir el riesgo para la seguridad de datos y comunicaciones", "emplear procedimientos apropiados y tecnologías disponibles, con preferencia a aquellos que han sido certificados, para proteger la privacidad de las personas afectadas (...), especialmente mediante la garantía de la integridad y confidencialidad de los datos, además de la seguridad física y lógica de la red" e informar a los usuarios de Internet sobre los modos de "usar sus servicios y pagar por ellos de forma anónima". Los suscriptores deberían tener acceso a una línea directa que les permitiese informar sobre violaciones a la privacidad, y los proveedores deberían suscribirse a un código de conducta que les obligase a bloquear el acceso a sitios web que no alcanzasen a cumplir con los requisitos de protección de datos, sin importar dónde esté localizada la página web.

El segundo objetivo está conformado por los fabricantes y desarrolladores de equipamiento y programas, y aquellos responsables del trazado de estándares técnicos y protocolos usados en la transmisión de información de la red. Deberían garantizar que sus productos o estándares:[26]

- cumplen la ley, por ejemplo garantizando que los navegadores de Internet transmiten la información mínima necesaria para conectar y adoptar medidas de seguridad apropiadas;
- facilitan la aplicación de los principios subrayados en la parte II, por ejemplo, permitiendo a los usuarios el acceso directo a sus datos personales y al ejercicio del derecho de objeción automático, en particular mediante el uso de blogs;
- elevan el nivel de protección de datos personales.

25. Quizás, en la misma línea, debemos ampliar el alcance de la protección con respecto a los datos cubiertos por las legislaciones de privacidad. Las nuevas tecnologías hacen progresivamente posible el procesamiento de datos en relación con individuos, no, como en el caso tradicional, mediante datos relacionados a su identidad legal como el nombre o dirección, sino mediante un punto de anclaje o incluso un objeto (llamado inteligencia ambiente) asociado. Los datos generados por cookies, al igual que los generados por las etiquetas RFID incrustadas en la ropa o en productos, no hacen necesariamente referencia a un individuo, sino que, como permiten contactar e incluso tomar decisiones respecto de una persona, la persona tras el terminal en el caso de los cookies o la persona poseedora de la ropa o los productos en el caso de RFID, debe estar sujeta a determinada protección.

26. Los terminales, en el amplio sentido, deben convertirse en herramientas tecnológicas totalmente transparentes para aquellos que las tienen y las usen. Es más, en muchos casos en realidad pertenecen a los individuos interesados y podrían verse como parte de su hogar. Cualquier intrusión en su privacidad debe ser tratada como cualquier otra intrusión.

La opacidad y complejidad de los sofisticados sistemas de información a los que las personas someten datos requieren información adicional que ya no se centra estrictamente en el procesamiento en sí o en características individuales, sino en el funcionamiento general del sistema de información y su habilidad para generar una vasta cantidad de información, presente y futura. De ahí la necesidad de documentar los datos (origen, usuarios, justificación lógica), describir los diversos flujos de información y sentar normas que controlen cómo se toman las decisiones, quién tiene acceso y cómo se controla.

Hasta ahora, las autoridades de protección de datos tradicionalmente no han prestado atención a las herramientas tecnológicas. Raramente emplean especialistas informáticos o penetran en el sancta sanctorum de aquellos que deciden qué desarrollos tecnológicos se realizarán y cómo se configurarán los productos. Tal y como los Estados europeos han demandado el establecimiento de un Comité Asesor Gubernamental (GCA) al ICANN, un organismo privado responsable de la gestión de nombres y direcciones de dominios de Internet, podría ser igualmente necesario proponer o incluso insistir sobre un Comité Asesor de Protección de Datos al ICANN, W3C (Consorcio World Wide Web) y el IETF (Grupo de Trabajo en Ingeniería de Internet). Es necesario hacer que el sector de comunicaciones electrónicas sea plenamente consciente de la importancia de la protección de datos.

27. Para resumir, me gustaría destacar las dos necesidades principales siguientes:

- la necesidad de suministrar a los individuos todo lo que precisen para comprender y controlar su entorno informático; en particular, el medio de

26 Ver la opinión de la Comisión Belga n.º 34/2000 sobre comercio electrónico y protección de datos.

penetrar en sus hogares. Se les debe otorgar control sobre cualquier herramienta cuyo uso haga que se muestren a otros.

- la necesidad de dotar a la sociedad de herramientas para controlar los desarrollos tecnológicos, que de otro modo podrían amenazar la supervivencia de nuestras libertades colectivas e individuales.

La legislación vial impone a los usuarios determinadas normas no sólo para reducir los accidentes, sino también para alcanzar un equilibrio satisfactorio entre derechos y obligaciones de los diferentes usuarios de la carretera, estando las leyes inclinadas a ofrecer protección específica a los más vulnerables. Esto requiere no sólo un código vial sino legislación específica sobre la red de carreteras en sí y los vehículos que pueden usarlas, que están sujetos a determinados estándares obligatorios.

En la autopista de la información no existe una legislación que rija las normas de funcionamiento de las telecomunicaciones para la protección de la privacidad de los usuarios o requisitos para garantizar que los terminales de telecomunicación que facilitan a los usuarios navegar en esas autopistas funcionan con justicia y transparencia.

Tan sólo aplicando los principios de protección de datos tradicionales a estas nuevas tecnologías, que son implícitos pero componentes inevitables de toda telecomunicación, puede la computación dirigirnos a una sociedad de la información democrática, proporcionando progreso general para todos.